科学研究費助成事業　　研究成果報告書

平成　２６　年　　５　月　２７　日現在

機関番号：　１７４０１
研究種目：　基盤研究(C)
研究期間：　2011～2013
課題番号：　２３５６０４６０

研究課題名（和文）カオス理論とシフトレジスタに基づいた符号系列の設計と応用

研究課題名（英文）Design and Application of Code Sequences Based on Chaos Theory and Shift Registers

研究代表者
常田　明夫（TSUNEDA, Akio）

熊本大学・自然科学研究科・准教授

研究者番号：４０２７４４９３

交付決定額（研究期間全体）：（直接経費）　　4,000,000円、（間接経費）　　1,200,000円

研究成果の概要（和文）：本研究では，M系列やGold系列を生成する線形フィードバックシフトレジスタ（LFSR）およびその一般形である非線形フィードバックシフトレジスタ（NFSR）に，カオス理論に基づいて設計された組合せ論理回路を付加することで，非同期CDMA通信で有用な負相関スペクトル拡散符号が生成可能であることを明らかにした．また，提案系列を，光CDMA通信や測位システムに応用した場合の性能評価を行い，提案系列の有効性を明らかにした．

研究成果の概要（英文）：In this research, we designed binary sequences with negative auto-correlation based on LFSRs/NFSRs and the chaos theory and revealed that the proposed sequences can reduce bit error rate (BER) in asynchronous DS/CDMA systems compared with the conventional Gold sequences. Furthermore, it has been shown that the proposed spreading sequences are also useful for optical CDMA communications and local positioning systems.

研究分野：　工学

科研費の分科・細目：　電気電子工学、通信・ネットワーク工学

キーワード：　Gold系列　CDMA　非線形フィードバックシフトレジスタ　負相関系列　カオス理論　ユニポーラ符号　TDOA　屋内測位システム

１．研究開始当初の背景

スペクトル拡散(SS)通信技術に基づく符号分割多元接続(Code Division Multiple Access; CDMA)方式は，耐雑音性，耐マルチパスフェージング，周波数利用効率などの点で優れ，従来の FDMA（周波数分割多元接続）や TDMA（時分割多元接続）に代わる通信技術として第３世代携帯電話で実用化されている．CDMA システムの性能は，情報信号の帯域を拡散するために用いられる擬似乱数系列（スペクトル拡散符号）の自己相関特性や相互相関特性に大きく依存するので，現在まで様々な系列の設計が盛んになされてきている．

拡散符号に要求される性質として，チャネル間干渉の低減や同期捕捉のために自己・相互相関特性が良いこと，多くのユーザに割り当てることができるように多種類の符号が存在すること，安価でかつ小型のハードウェアで高速に生成可能であること，などが挙げられる．従来の拡散符号としては，M 系列やこれを基にした Gold 系列，Kasami 系列がよく知られており，これらは良好な相関特性を有するとともに，線形フィードバックレジスタ(LFSR)により高速に生成可能である．しかしながら，同じ長さの系列の種類数は限られており，より多くのユーザに対応できないという欠点がある．

一方，単純な決定論的システムから生じるランダムなカオス現象をスペクトル拡散符号に応用する試みが盛んに行われてきた．それらの多くは一次元写像から生成されるカオス系列を利用するものであり，1993 年に Kohda & Tsuneda によってカオス２値系列を拡散符号として利用する試みがなされて以来，多くの研究者がカオスに基づいたスペクトル拡散符号を提案している．カオス系列は確率的な振舞をし，用いる写像などに依存して，様々な性質を有するので，その統計的性質が理論的に解析可能であること，および所望の性質をもつ系列が設計可能であることが非常に重要である．

ある適切な負の自己相関特性をもつカオス系列を非同期 CDMA システムにおけるスペクトル拡散符号として用いると，従来のスペクトル拡散符号を用いた場合よりもビット誤り率が低減できることが Rovatti & Mazzini によって 1998 年に理論的に明らかにされた．また，彼らは，負の自己相関をもつ具体的なカオス系列の生成法も与えていた．本研究代表者も，独自の手法で負（あるいは正）の指数関数的に減衰する自己相関をもつカオス２値系列および p 値系列の設計法を与えており，この手法に基づくと，非同期 CDMA において理論的に最適とされる相関パラメータを厳密かつ容易に設定できる．カオス拡散符号は，初期値などのパラメータを変えることで，極めて多種類の符号が生成可能であり，その実用化が期待されている．

２．研究の目的

カオス符号は本来実数演算（すなわちアナログ演算）によって生成されるものであるが，送受信側における再現性のために，十分な精度のディジタル演算（有限ビット演算）により生成することが多い．当然，演算ビット数が多いほど，理論上のカオス符号の特性に近づくことが期待できるが，演算ビット数を増大させた場合，生成速度やコスト，および装置規模の点で，従来の LFSR 系列に比べて不利となるため，この点を克服することが実用化へ向けての１つの課題である．本研究代表者は，カオス系列の具体的生成回路の実現方法として，カオス写像を有限ビットで近似し，その精度で最大の周期をもつ最大周期系列を提案し，その諸特性を調査した．この考え方に基づけば，従来の LFSR およびこれを非線形に一般化した非線形フィードバックシフトレジスタ（NFSR）もカオス写像として有名なベルヌイ写像の近似の一つであると見なすこと出来る．さらに，ベルヌイ写像から CDMA で有用な負の自己相関をもつカオス２値系列を生成する方法を理論的に与え，写像の近似である LFSR/NFSR に簡素な回路を付け加えることで，負相関をもつ周期２値系列が生成可能であり，従来符号よりも低いビット誤り率を達成可能であることを確認した．

本研究では，上述のこれまでの成果，すなわち，カオス理論に基づいた符号設計が LFSR/NFSR 系列設計にも有効であることに基づき，次世代の CDMA 通信や近距離通信（超音波測位システム，可視光通信）において有用な符号生成器の実現を目的とする．

３．研究の方法

(1)M系列は同じ長さの系列の種類が極めて少ないため，このまま CDMA 用のスペクトル拡散符号としては利用し難い．１つのM系列から６つの２値関数（論理関数）を用いることで，６種類の負相関系列を生成可能であることを既に明かにしており，これらはM系列を生成する LFSR の上位３ビットを用いて３入力１出力の論理関数として構成される．そこで，上位３ビットを４ビット以上に拡張することにより，さらに多くの負相関系列を生成できるかどうか検討する．

(2)非同期 DS/CDMA 通信で有用な負相関スペクトル拡散符号は，一次元カオス写像を利用することによって生成可能であるが，一般に，その符号生成器は従来の LFSR（線形フィードバックシフトレジスタ）よりも複雑で高価となる．本研究では，LFSR 回路により生成される Gold 系列を，カオス理論に基づいて構成した論理関数を用いて負相関系列に変換する手法を提案し，提案系列を用いて，加法性白色ガウス雑音（AWGN）環境下や位相雑音を考慮した場合の非同期 DS/CDMA 通信シミュレーションを行い，そのビット誤り率（BER）特性を評価する．

(3)電波を用いたCDMA通信における２値のスペクトル拡散符号は通常 1 と-1 の信号を用いるバイポーラ符号を用いているが，光通信においては，光の点滅により通信を行うため，1 と 0 のユニポーラ符号として利用する必要がある．ユニポーラ符号を用いた光CDMA 通信方式として,バイポーラ符号の相関特性を活かせる SIK(sequence inversion keyed)方式が提案されており，NFSR（非線形フィードバックレジスタ）系列および Gold 系列を用いた SIK 方式光 CDMA 通信の性能をシミュレーションにより評価する．
(4) オンオフキーイング CDMA 方式と TDOA（time difference of arrival）を用いた超音波による測位システムを想定し，Gold 系列および NFSR 直交系列をスペクトル拡散符号として用いた場合の測位シミュレーションを行い，各系列を用いた場合の相関受信機の出力特性，同期点検出能力，および測位精度について評価する．また，超音波送受信モジュールと FPGA を用いて簡易実験を行う．

４．研究成果
(1)M系列を生成する LFSR の上位４ビットを用いて４入力１出力の論理関数を構成することにより，さらに多くの負相関系列を生成できるかどうか検討した．その結果，24 個の２値関数があり，一つのM系列から 24 個の負相関系列が生成できることを明らかにした．さらに，この提案系列を非同期 DS/CDMA 通信におけるスペクトル拡散符号として用いた場合，従来の Gold 系列よりもビット誤り率が低減できることを明らかにした．
(2)LFSR 回路により生成される Gold 系列を，カオス理論に基づいて構成した論理関数を用いて負相関系列に変換する手法を提案し，提案系列が，加法性白色ガウス雑音（AWGN）環境下や位相雑音を考慮した場合の非同期 DS/CDMA 通信において，元の Gold 系列やM系列よりも低いビット誤り率（BER）特性を示すことを明らかにした．
(3)NFSR（非線形フィードバックレジスタ）系列および Gold 系列を用いた SIK 方式光 CDMA 通信の性能を評価した結果，SIK 方式 CDMA の場合，NFSR に基づいた系列は，バイポーラの場合と同様，負相関化することで元の無相関系列よりも低い BER を達成したが，Gold 系列の場合は，バイポーラの場合よりも BER 特性が極端に悪化することを明らかにした．これは，0 と 1 のバランス性に起因するものだと考えられる．さらに，既存の光 CDMA 用符号であるプライム符号とも比較検討し，負相関化した NFSR 系列の有効性を明らかにした．
(4) オンオフキーイング CDMA 方式と TDOA を用いた超音波による測位システムを想定し，Gold 系列および NFSR 直交系列をスペクトル拡散符号として用いた場合の測位シミュレーションを行い，各系列を用いた場合の相関受信機の出力特性，同期点検出能力，および測位精度について評価した．その結果，非平衡 Gold 系列では，同期点のピーク値が低くなっているものがあり，用いる符号は平衡系列が望ましく，また，ｃｍオーダの測位のためには，チップレートを 10kcps 程度以上にする必要があることを明らかにした．また，超音波送受信モジュールを用いて簡易実験を行い，提案方式による符号の送受信ができることを確認した．

５．主な発表論文等

〔雑誌論文〕（計１３件）
(1) D.Yoshioka and A.Tsuneda, “The design of low complexity S-boxes based on a discretized piecewise linear chaotic map,” IEICE Trans. Fundamentals, Vol.E97-A, No.6, Jun. 2014（掲載決定）, 査読有.
(2) A.Tsuneda and K.Morikawa, “A Study on Random Bit Sequences with Prescribed Auto-Correlations by Post-Processing Using Linear Feedback Shift Registers,” Proc. of 2013 European Conference on Circuit Theory and Design, Sep. 2013, 査読有.
(3) D.Yoshioka, “Hardware implementable S-box based on a discretized piecewise linear chaotic map,” Proc. of 9th IEEE International Wireless Communications & Mobile Computing Conference, pp.1120-1125, Jul. 2013, 査読有
(4) Y.Kawano and A.Tsuneda, “Performance Evaluation of Indoor Positioning Systems Based on On-Off Keying CDMA and TDOA,” Proc. of 2013 International Tech. Conf. on Circuits/Systems, Computers and Communications, pp.446-449, Jun. 2013, 査読有.
(5) S.Abe and A.Tsuneda, “Performance Evaluation of Spreading Codes with Negative Auto-Correlation Based on Gold Sequences and Chaos Theory －BER in Asynchronous DS/CDMA Communications under AWGN Environment－,” Proc. of 2013 International Tech. Conf. on Circuits/Systems, Computers and Communications, pp.450-453, Jun. 2013, 査読有.
(6) S.Araki and A.Tsuneda, “BER Evaluation of Asynchronous SIK Optical CDMA Communications Using Spreading Codes with Negative Auto-Correlation,” Proc. of 2013 International Tech. Conf. on Circuits/Systems, Computers and Communications, pp.972-975, Jun. 2013, 査読有.
(7) D.Yoshioka, “Design of a Low

Complexity S-Box Based on a Piecewise Linear Chaotic Map," Proc. of 19th IEEE International Conference on Electronics, Circuits, and Systems, pp.853-856, Dec. 2012, 査読有.
(8) K.Fukuda and A.Tsuneda, "Key-Sensitivity Improvement of Block Cipher Systems Based on Nonlinear Feedback Shift Registers," Proc. of 2012 IEEE Asia Pacific Conference on Circuits and Systems, pp.100-103, Dec. 2012, 査読有.
(9) A.Tsuneda and S.Inada, "Study on Auto-Correlation Functions of Low-Density Binary Sequences Generated by Bernoulli Map and Nonlinear Feedback Shift Registers," Proc. of 2012 International Symposium on Nonlinear Theory and its Applications, pp.895-898, Oct. 2012, 査読有.
(10) A.Tsuneda and T.Yoshida, "Performance Evaluation of Asynchronous DS/CDMA Communications Using Unipolar Codes," Proc. of 2011 European Conference on Circuit Theory and Design, pp.669-672, Aug. 2011, 査読有.
(11) S.Tokunaga and A.Tsuneda, "A Study on Spreading Sequences with Negative Auto-Correlation Based on Chaos Theory and M-Sequences," Proc. of 2011 International Tech. Conf. on Circuits/Systems, Computers and Communications, pp.866-869, Jun. 2011, 査読有.
(12) S.Matsuo and A.Tsuneda, "Aperiodic Correlation Properties of Pseudorandom Binary Sequences as Unipolar Codes －Comparison of NFSR Orthogonal Sequences and Gold Sequences －," Proc. of 2011 International Tech. Conf. on Circuits/Systems, Computers and Communications, pp.874-877, Jun. 2011, 査読有.
(13) D.Yoshioka and A.Tsuneda, "Design of Maximum Length Pseudochaotic Sequences Derived from Discretized 1-D Chaotic Maps and Their Autocorrelation Properties," IEICE Trans. Fundamentals, vol.E94-A, no.6, pp.1408-1416, Jun. 2011, 査読有.

〔学会発表〕(計３５件)
(1) 吉岡大三郎, "テント型シフト写像に基づく S-box の設計と評価," 2014 年暗号と情報セキュリティシンポジウム(SCIS), 2014 年 1 月 23 日, 鹿児島市.
(2) 台信雄太, 吉岡大三郎, "２べき剰余環上のチェビシェフ多項式から得られる系列の周期," 2014 年暗号と情報セキュリティシンポジウム(SCIS), 2014 年 1 月 21 日, 鹿児島市.
(3) 常田明夫, "カオス理論に基づいた符号・乱数の設計と応用," 第 283 回 RIST フォーラム, 2013 年 11 月 21 日, 熊本市.
(4) 森川晃大, 常田明夫, "カオス理論に基づいた後処理による非周期 2 値乱数系列の自己相関特性," 平成 25 年度電気関係学会九州支部連合大会, 2013 年 9 月 25 日, 熊本市.
(5) 村上晋介, 常田明夫, "直交 2 値系列を用いた SIK 方式光 CDMA 通信の BER 特性," 平成 25 年度電気関係学会九州支部連合大会, 2013 年 9 月 25 日, 熊本市.
(6) 福田光太郎, 常田明夫, NFSR に基づいた 64 ビットブロック暗号システムの鍵感度向上," 平成 25 年度電気関係学会九州支部連合大会, 2013 年 9 月 25 日, 熊本市.
(7) 許斐亜斗, 福田光太郎, 常田明夫, "NFSR ブロック暗号システムの鍵設定法と鍵感度に関する一検討," 第 21 回電子情報通信学会九州支部学生会講演会, 2013 年 9 月 23 日. 熊本市.
(8) 石堂宏樹, 常田明夫, "(2N,N)線形ブロック符号の最小重みに関する一検討," 第 21 回電子情報通信学会九州支部学生会講演会, 2013 年 9 月 23 日. 熊本市.
(9) 馬場崎公平, 阿部怜史, 常田明夫, "非同期 DS/CDMA 通信における相関受信機出力の分布について," 第 21 回電子情報通信学会九州支部学生会講演会, 2013 年 9 月 23 日. 熊本市.
(10) 春山慎太郎, 河野悠樹, 常田明夫, "Barker 系列と NFSR 系列による積符号の非周期自己相関特性," 第 21 回電子情報通信学会九州支部学生会講演会, 2013 年 9 月 23 日. 熊本市.
(11) 森川晃大, 常田明夫, "カオス理論に基づいた後処理による 2 値乱数の自己相関特性," 電子情報通信学会回路とシステム研究会, 2013 年 7 月 12 日, 熊本市.
(12) 村上晋介, 常田明夫, 直交 2 値系列を用いた SIK 方式光 CDMA 通信の一検討," 電子情報通信学会回路とシステム研究会, 2013 年 7 月 12 日, 熊本市.
(13) 吉岡大三郎, "区分線形写像に基づく S-box の設計とその実装," 2013 年電子情報通信学会総合大会, 2013 年 3 月 21 日, 岐阜市.
(14) 阿部怜史, 常田明夫, "Gold 系列とカオス理論に基づいた負相関スペクトル拡散符号の性能評価～AWGN 環境下での非同期 DS/CDMA 通信の BER 特性～," 電子情報通信学会回路とシステム研究会, 2013 年 1 月 29 日, 別府市.
(15) 荒木誠司, 常田明夫, "負相関スペクトル拡散符号を用いた SIK 方式非同期光 CDMA 通信の BER 特性," 電子情報通信学会回路とシステム研究会, 2013 年 1 月 29 日, 別府市.
(16) 河野悠樹, 常田明夫, "オンオフキーング CDMA と TDOA に基づいた屋内測位システムの性能評価," 電子情報通信学会回路と

システム研究会, 2013 年 1 月 29 日, 別府市.
(17) 徳永昌平, 常田明夫, “M 系列とカオス理論に基づいた負相関スペクトル拡散符号の性能評価,” 電子情報通信学会回路とシステム研究会, 2013 年 1 月 28 日, 別府市.
(18) 森川晃大, 常田明夫, “カオス理論に基づいた後処理による非周期２値乱数の自己相関の変化,” 第 20 回電子情報通信学会九州支部学生会講演会, 2012 年 9 月 26 日, 長崎市.
(19) 岡部由季, 吉岡大三郎, “整数値の区分線形カオス写像に基づく Sbox の設計とその差分確率の評価,” 第 20 回電子情報通信学会九州支部学生会講演会, 2012 年 9 月 26 日, 長崎市.
(20) 梅原健志郎, 常田明夫, “NFSR 系列に基づいた線形ブロック符号の最小距離について,” 第 20 回電子情報通信学会九州支部学生会講演会, 2012 年 9 月 26 日, 長崎市.
(21) 川口安司, 河野悠樹, 常田明夫, “一般化相関関数とオンオフキーイング CDMA に基づいた屋内測位システムの一検討,” 第 20 回電子情報通信学会九州支部学生会講演会, 2012 年 9 月 26 日, 長崎市.
(22) 村上晋介, 荒木誠司, 常田明夫, “直交２値系列を用いた SIK 方式光 CDMA 通信の一検討,” 第 20 回電子情報通信学会九州支部学生会講演会, 2012 年 9 月 26 日, 長崎市.
(23) 阿部怜史, 常田明夫, “AWGN 環境下の非同期 DS/CDMA 通信における負相関スペクトル拡散符号の BER 特性,” 平成 24 年度電気関係学会九州支部連合大会, 2012 年 9 月 24 日), 長崎市.
(24) 荒木誠司, 常田明夫, “SIK 方式非同期光 CDMA 通信用スペクトル拡散符号の特性評価,” 平成 24 年度電気関係学会九州支部連合大会, 2012 年 9 月 24 日), 長崎市.
(25) 河野悠樹, 常田明夫, “オンオフキーイング CDMA 方式と TDOA を用いた屋内測位システムの一検討,” 平成 24 年度電気関係学会九州支部連合大会, 2012 年 9 月 24 日), 長崎市.
(26) 福田光太郎, 常田明夫, “NFSR ブロック暗号システムの鍵感度向上に関する検討,” 電子情報通信学会回路とシステム研究会, 2012 年 1 月 19 日, 福岡市.
(27) 徳永昌平, 常田明夫, “M 系列とカオス理論に基いた負相関スペクトル拡散符号の生成と評価,” 電子情報通信学会回路とシステム研究会, 2012 年 1 月 19 日, 福岡市.
(28) 稲田翔吾, 常田明夫, “ベルヌイ写像から生成される低密度カオス２値系列の自己相関特性,” 第 19 回電子情報通信学会九州支部学生会講演会, 2011 年 9 月 28 日, 佐賀市.
(29) 阿部怜史, 常田明夫, “Gold 系列とカオス理論に基づいた負相関スペクトル拡散符号の性能～AWGN 環境下での非同期 DS/CDMA 通信のビット誤り率評価～,” 第 19 回電子情報通信学会九州支部学生会講演会, 2011 年 9 月 28 日, 佐賀市.
(30) 荒木誠司, 常田明夫, “SIK 方式光 CDMA 通信用スペクトル拡散符号の相関特性～NFSR 系列と Gold 系列の比較～,” 第 19 回電子情報通信学会九州支部学生会講演会, 2011 年 9 月 28 日, 佐賀市.
(31) 河野悠樹, 常田明夫, “オンオフキーング CDMA に基づいた屋内測位システムの一検討,” 第 19 回電子情報通信学会九州支部学生会講演会, 2011 年 9 月 28 日, 佐賀市.
(32) 常田明夫, “区分線形写像から生成される低密度カオス２値系列の自己相関関数,”平成 23 年度電気関係学会九州支部連合大会, 2011 年 9 月 27 日, 佐賀市.
(33) 徳永昌平, 常田明夫, “M系列とカオス理論に基づいた負相関スペクトル拡散符号の特性評価,” 平成 23 年度電気関係学会九州支部連合大会, 2011 年 9 月 27 日, 佐賀市.
(34) 福田光太郎, 常田明夫, “NFSR ブロック暗号システムの鍵感度向上に関する考察,” 平成 23 年度電気関係学会九州支部連合大会, 2011 年 9 月 27 日, 佐賀市.
(35) 井上祐鷹, 常田明夫, “Walsh 直交関数に基づいた論理回路による非周期２値乱数の後処理の効果,” 平成 23 年度電気関係学会九州支部連合大会, 2011 年 9 月 27 日, 佐賀市.

６．研究組織

(1)研究代表者

常田　明夫（TSUNEDA, Akio）
熊本大学・大学院自然科学研究科・准教授
研究者番号：４０２７４４９３

(2)研究分担者

吉岡　大三郎（YOSHIOKA, Daisaburo）
崇城大学・情報学部・准教授
研究者番号：　７０４３５１４７